Deployment and Operations

Description

The objective of this content area is to describe (and provide pointers to) commonly accepted best practices and processes and relevant characteristics of organizations that are demonstrating competence in sustaining adequate security during deployment and operations. Armed with this information, you can better determine which practices are most applicable to the deployment and operations of your own software and systems.

Articles in this Content Area

Overview Article: Deploying and Operating Secure Systems[1]

Article 1: Plan, Do, Check, Act[2] (PDCA) describes a general approach to security improvement that can be applied equally well to an individual practice or control or to a full-blown information security architecture and management system. It

- describes prerequisites that need to be in place for an effective, sustainable security effort
- presents a table of minimum essential practices required for basic security hygiene that serve as the foundation for any subsequent effort
- introduces several implementation frameworks

This PDCA approach can be used to deploy and operate the categories of practices described in the other articles in this content area.

Article 2: Risk-Centered Practices[3] further describes candidate practices that produce the risk assessment results prerequisite called out in Plan, Do, Check, Act[4]. Given that it is impractical (and likely impossible) to ensure that an operational system and all of its software are 100% secure at any point in time, security practitioners have found it useful to adopt risk management and assessment approaches to determine which security practices to deploy and in what order.

Article 3: Integrating Security and IT[5] describes effective ways to address security controls in an IT operational environment. Practitioners responsible for deploying and operating systems with high availability and security requirements accomplish this, in part, by embedding well-defined security controls in mature IT operational processes, such as change management, configuration management, and release management.

Article 4: Prioritizing IT Controls for Effective Security[6] summarizes results from the *IT Controls Performance Study* conducted by the IT Process Institute[7]. The article describes what differentiates high performing organizations in IT and security from others and identifies six foundational controls that are deployed by these organizations.

Article 5: Navigating the Security Practice Landscape[8] presents a summary of the leading sources of security practice definition and implementation guidance. It uses ISO 17799 as a foundation (given its international standard status and broad, installed base) and builds upon and augments it with additional source material. A summary of publicly available CERT course materials is presented to aid in practice

[1] http://buildsecurityin.us-cert.gov/bsi/articles/best-practices/deployment/218-BSI.html (Deploying and Operating Secure Systems)

[2] http://buildsecurityin.us-cert.gov/bsi/articles/best-practices/deployment/574-BSI.html (Plan, Do, Check, Act)

[3] http://buildsecurityin.us-cert.gov/bsi/articles/best-practices/deployment/575-BSI.html (Risk-Centered Practices)

[4] http://buildsecurityin.us-cert.gov/bsi/articles/best-practices/deployment/574-BSI.html (Plan, Do, Check, Act)

[5] http://buildsecurityin.us-cert.gov/bsi/articles/best-practices/deployment/576-BSI.html (Integrating Security and IT)

[6] http://buildsecurityin.us-cert.gov/bsi/articles/best-practices/deployment/577-BSI.html (Prioritizing IT Controls for Effective, Measurable Security)

[7] http://www.itpi.org/

[8] http://buildsecurityin.us-cert.gov/bsi/articles/best-practices/deployment/582-BSI.html (Navigating the Security Practice Landscape)

implementation. The content in this article can be used independently or in concert with the approaches described in the other articles in this content area.

Most Recently Updated Articles [Ordered by Last Modified Date]

Name	Version Creation Time	Abstract
Deployment and Operations References	1/6/10 2:52:42 PM	Content area bibliography.
Navigating the Security Practice Landscape	2/6/09 11:46:58 AM	This article presents a summary of ten leading sources of security practice definition and implementation guidance. It uses ISO 27002 as a foundation (given its international standard status and broad, installed base) and builds on and augments it with additional source material. A summary of publicly available CERT course materials is presented to aid in practice implementation. The content in this article can be used independently or in concert with the approaches described in the other articles in this content area.
Risk-Centered Practices	1/7/09 11:07:39 AM	This article establishes the role that risk management and risk assessment play in determining what security practices to implement and in what order. Risk management is critical in sustaining an acceptable level of security, given that it is not possible to be 100% secure.
Deploying and Operating Secure Systems	1/6/09 4:17:02 PM	This article provides a brief overview of deployment and operations security issues, notes to the reader to set expectations, and a recommended order for using the practices described in this content area.
Integrating Security and IT	1/6/09 4:01:41 PM	This article describes the key relationship between IT processes and security controls. Most, if not all, IT processes play a critical role in sustaining a desired security state during deployment and operations.

All Articles [Ordered by Title]

Name	Version Creation Time	Abstract
Deploying and Operating Secure Systems	1/6/09 4:17:02 PM	This article provides a brief overview of deployment and operations security issues, notes to the reader to set expectations, and a recommended order for using the practices described in this content area.
Deployment and Operations References	1/6/10 2:52:42 PM	Content area bibliography.
Integrating Security and IT	1/6/09 4:01:41 PM	This article describes the key relationship between IT processes and security controls. Most, if not all, IT processes play a critical role in sustaining a desired security state during deployment and operations.
Navigating the Security Practice Landscape	2/6/09 11:46:58 AM	This article presents a summary of ten leading sources of security practice definition and implementation guidance. It uses ISO 27002 as a foundation (given its international standard status and broad, installed base) and builds on and augments it with additional source material. A summary of publicly available CERT course materials is presented to aid in practice implementation. The content in this article can be used independently or in concert with the approaches described in the other articles in this content area.
Plan, Do, Check, Act	12/30/08 4:48:25 PM	This article describes a tried and true approach to security improvement that can be effectively used during deployment and operations. It identifies prerequisites that must be in place to sustain a desired state of security. It provides a set of minimum requirements for security hygiene and several security implementation frameworks that can be used in concert with the other articles in this content area.

Prioritizing IT Controls for Effective, Measurable Security	1/2/09 10:42:23 AM	This article summarizes results from the *IT Controls Performance Study* conducted by the IT Process Institute[9]. The article describes what differentiates high performing organizations in IT and security from others and identifies six foundational controls that are deployed by these organizations.
Risk-Centered Practices	1/7/09 11:07:39 AM	This article establishes the role that risk management and risk assessment play in determining what security practices to implement and in what order. Risk management is critical in sustaining an acceptable level of security, given that it is not possible to be 100% secure.